Formal Methods and Functional Programming

Natural Semantics

Peter Müller

Chair of Programming Methodology
ETH Zurich

Natural Semantics of IMP

- Skip

$$\frac{}{\langle \texttt{skip}, \sigma \rangle \to \sigma} \; (\textsc{Skip}_{NS})$$

- Assignment

$$\frac{}{\langle x := e, \sigma \rangle \to \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma]} \; (\textsc{Ass}_{NS})$$

- Sequential Composition

$$\frac{\langle s, \sigma \rangle \to \sigma' \quad \langle s', \sigma' \rangle \to \sigma''}{\langle s; s', \sigma \rangle \to \sigma''} \; (\textsc{Seq}_{NS})$$

Natural Semantics of IMP (cont'd)

- Conditional

$$\frac{\langle s, \sigma\rangle \to \sigma'}{\langle \texttt{if } b \texttt{ then } s \texttt{ else } s' \texttt{ end}, \sigma\rangle \to \sigma'}\ (\textsc{IfT}_{NS}) \quad \text{if } \mathcal{B}[\![b]\!]\sigma = tt$$

$$\frac{\langle s', \sigma\rangle \to \sigma'}{\langle \texttt{if } b \texttt{ then } s \texttt{ else } s' \texttt{ end}, \sigma\rangle \to \sigma'}\ (\textsc{IfF}_{NS}) \quad \text{if } \mathcal{B}[\![b]\!]\sigma = ff$$

- Loop

$$\frac{\langle s, \sigma\rangle \to \sigma' \quad \langle \texttt{while } b \texttt{ do } s \texttt{ end}, \sigma'\rangle \to \sigma''}{\langle \texttt{while } b \texttt{ do } s \texttt{ end}, \sigma\rangle \to \sigma''}\ (\textsc{WhT}_{NS}) \quad \text{if } \mathcal{B}[\![b]\!]\sigma = tt$$

$$\frac{}{\langle \texttt{while } b \texttt{ do } s \texttt{ end}, \sigma\rangle \to \sigma}\ (\textsc{WhF}_{NS}) \quad \text{if } \mathcal{B}[\![b]\!]\sigma = ff$$

Natural Semantics: Extensions

- Local Variables

$$\frac{\langle s, \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma]\rangle \to \sigma'}{\langle \texttt{var } x\texttt{:=}e \texttt{ in } s \texttt{ end}, \sigma\rangle \to \sigma'[x \mapsto \sigma(x)]} \ (\textsc{Loc}_{NS})$$

- Procedures

$$\frac{\langle s, \sigma_{zero}[\overrightarrow{x_i} \mapsto \overrightarrow{\mathcal{A}[\![e_i]\!]\sigma}][\overrightarrow{y_j} \mapsto \overrightarrow{\sigma(z_j)}]\rangle \to \sigma'}{\langle p(\overrightarrow{e_i}\,;\overrightarrow{z_j}), \sigma\rangle \to \sigma[\overrightarrow{z_j} \mapsto \overrightarrow{\sigma'(y_j)}]} \ (\textsc{Call}_{NS})$$

- Non-determinism

$$\frac{\langle s, \sigma\rangle \to \sigma'}{\langle s \,[\!]\, s', \sigma\rangle \to \sigma'} \ (\text{ND1}_{NS}) \qquad \frac{\langle s', \sigma\rangle \to \sigma'}{\langle s \,[\!]\, s', \sigma\rangle \to \sigma'} \ (\text{ND2}_{NS})$$